IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

First Named Inventor:

Guo Liang Yang

Application No.: 10/580,776

Filed: May 26, 2006

For: A METHOD AND APPARATUS FOR BUILDING A MULTI-DISCIPLINE AND MULTI-MEDIA PERSONAL MEDICAL IMAGE LIBRARY NETWORK

Examiner: Vo, Cecile H.

Art Unit: 2169

Confirmation No.: 7128

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below.

/Betty Scaletta/ 06-22-2011

Betty Scaletta **Date**

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37(a)

This is an appeal to the Board of Patent Appeals and Interferences from the decision of the Examiner of Group 2169 mailed December 7, 2010 which finally rejected claims 1-4, 6, and 8-37 in the above-identified application. The Office's date of receipt of Appellants' Notice of Appeal was March 7, 2011. The Notice of Panel Decision from Pre-Appeal Brief Review was mailed on April 22, 2011. This Appeal Brief is hereby submitted pursuant to 37 C.F.R. § 41.37(a). The Petition for Extension of Time pursuant to 37 C.F.R. § 1.136 (a) is filed herewith.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real parties in interest are Agency for Science, Technology, and Research and National Neuroscience Institute, corporations of Singapore, the assignees of record having principle places of business at 20 Biopolis Way, #07-01, Centros, Singapore, 138668 and 11 Jalan Tan Tock Seng, Singapore, 308433 respectively.

II. RELATED APPLEALS AND INTERFERENCES

To the best of Appellants' knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF CLAIMS

Claims 1-4, 6, and 8-37 are pending in the present application. Claims 5 and 7 have been canceled.

Claims 1-4, 6, and 8-37 were finally rejected under 35 U.S.C. §103(a) in an Office Action mailed December 7, 2010 (hereinafter "Office Action").

Claims 1-4, 6, and 8-37 are the subject of this appeal. A copy of claims 1-4, 6, and 8-37 as they stand on appeal is provided in the Claims Appendix.

IV. STATUS OF AMENDMENTS

No amendments have been submitted subsequent to the Office Action mailed December 7, 2010.

V. SUMMARY OF CLAIMED SUBJECT MATTER

This section of this Appeal Brief is set forth to comply with the requirements of 37 C.F.R. 41.37(c)(1)(v) and is not intended to limit the scope of the claims in any way. Exemplary implementations of the limitations of claims 1-4, 6, and 8-37 are described below.

Claim 1

Independent claim 1 describes a method for retrieving medical images from various sources and in different formats, to enable the creation of teaching files and research datasets, for the building of a personal medical image library (see page 3, line 36 – page 4, line 2), comprising (a) directly retrieving a plurality of medical images from various sources (see page 4, line 3 and page 7, lines 28-29); (b) storing the plurality of medical images in a database (see page 4, line 4 and page 7, lines 30-31); (c) generating a database record for the teaching files and research datasets (see page 4, line 5 and page 7, lines 31-32); (d) generating the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the teaching files and research datasets being compliant with at least one predetermined schema (see page 4, line 6 and page 12, line 8-page 13, line 14); (e) saving the teaching files and research datasets into the database (see page 4, line 7 and page 13, lines 16-17); (f) generating at least one index of the teaching files and research datasets (see page 4, line 8 and page 7, lines 33-34); (g) automatically anonymizing patient identification data when the at

least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code (see page 4, lines 19-23 and page 10, line 6-page 11, line 1); and (h) securely storing a relationship between the anonymization code and the patient identification data in a table in the database (see page 11, lines 1-8 and Fig. 4, operation 47).

Claim 2

According to dependent claim 2, the method further includes a searching mechanism for searching the teaching files and research datasets (see page 4, lines 10-11 and page 7, lines 34-35).

Claim 3

According to dependent claim 3, the medical images are from at least one discipline selected from the group consisting of: radiology, nuclear medicine, dermatology, pathology, ophthalmology, cardiology, neurology, endoscopy, angiography, biomedicine, ECG, EEG, and EMG (see page 4, lines 13-15 and page 7, lines 34-35).

Claim 4

According to dependent claim 4, the method is in accordance with MIRC schema (see page 4, line 17).

Claim 6

According to dependent claim 6, the patient identification data is able to be revealed to a generator of the teaching files and research datasets (see page 4, lines 19-21).

Claim 8

According to dependent claim 8, the anonymization code includes a prefix, a randomly generated number and a type (see page 4, lines 23-24 and page 10, lines 9-11).

Claim 9

According to dependent claim 9, the prefix is a short string of characters representing the generator of the sensitive information; and the type represents nature of the sensitive information (see page 4, lines 24-26 and page 10, lines 13-21).

Claim 10

According to dependent claim 10, a check is first performed to determine if the item of sensitive information has previously been anonymized and the anonymization code previously generated; and, if yes, retrieving and using the previously generated anonymization code (see page 4, lines 28-30, page 10, lines 31-34, Fig. 4).

Claim 11

According to dependent claim 11, the sensitive information includes one or more items selected from the group consisting of: patient's name, patient ID, other patient's names, other patient IDs, patient's birth name, patient's address, patient's telephone numbers, patient's

mother's birth name, region of residence, country of residence, military rank, branch of service, patient comments, additional patient history, referring physician's name, referring physician's address, referring physician's telephone number, and all other person names (see page 4, lines 32-37 and page 11, lines 14-32).

Claim 12

According to dependent claim 12, in step (c) of claim 1, ACR codes are entered as a result of system prompts (see page 5, line 1).

Claim 13

According to dependent claim 13, wherein the ACR codes are used for the at least one index of the teaching files (see page 5, lines 1-2).

Claim 14

According to dependent claim 14, indexing is by at least one selected from a group consisting of: title, abstract, keywords, authors, affiliations, contacts, patient information, radiological codes, image format, image compression status, image modality, anatomic location, and ACR codes (see page 5, lines 5-7).

Claim 15

According to dependent claim 15, for internal searching, patient sensitive information is revealed, and for external searching patient sensitive information is anonymized (see page 5, lines 9-10).

Claim 16

According to dependent claim 16, after each medical image is retrieved in step (a) it can be viewed before being stored (see page 9, lines 26-28).

Claim 17

According to dependent claim 17, all medical images are kept in their original format once retrieved (see page 9, lines 16-17).

Claim 18

According to dependent claim 18, the formats of the medial images include at least one selected from the group consisting of AVW, HDR/IMG (Analyze format version 8.0 and 7.5), BMP (Windows Bitmap format), DICOM (Digital Imaging and Communications in Medicine), GIF, JPEG, JPEG 2000, PNG, PNM, PPG, RGB, RGBA, SGI, TIFF, AVW, HDR/IMG (Analyze format: version 8.0 and 7.5), Animated GIF, MIRA, Mut-sliced TIFF, MOV, AVI, MP3, RM, and Waveform for ECG, EEG, EMG (see page 8, lines 19-page 9, line 13).

Claim 19

According to dependent claim 19, for two-dimensional medical images, two additional JPEG images are generated for ease of browsing using a web browser; and other image formats, an additional thumbnail image is generated (see page 9, lines 17-20).

Claim 20

According to dependent claim 20, the two additional JPEG images are of the same size as thumbnail images (see page 9, lines 18-19).

Claim 21

Claim 21 claims corresponding subject matter to claim 1 and is supported in the same sections of the specification.

Independent claim 21 describes an apparatus for retrieving medical images from various sources and in various formats for creating at least one teaching file and research dataset (see page 5, lines 12-14). The apparatus comprises a database (1, Figure 1) for storing the at least one teaching file and research dataset in a generated database record (see page 5, lines 14-16 and page 7, lines 5-6); an image retrieval interface (2, Figure 1) configured to directly retrieve medical images from various sources and in different formats (see page 5, lines 14-16 and page 7, lines 5-6); an MIRC server (3, Figure 1) configured to provide an MIRC file storage service for the database and for a user's machine automatically anonymizing patient identification data based upon the at least one medical image retrieved from the various sources, wherein the patient information data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code (see page 4, lines 19-23 and page 10, line 6-page 11, line 1), and wherein a relationship between the anonymization code and the patient identification data is stored securely in a table in the database (see page 6, lines 1-3 and page 7, lines 24-26); a graphic user interface (5, Figure 1) for operation on a user's machine to communicate with the MIRC server (see page 5, lines 16-17 and lines 35-37); and a web server

(4, Figure 1) to service requests from the graphic user interface (see page 5, lines 23-24 and page 7, line 9).

Claim 22

According to dependent claim 22, the database is a relational database for storage of all required information, including: database tables, database indexes, database scripts; and pointers to the medical images, teaching files and research datasets (see page 5, lines 19-21 and page 7, lines 1-3).

Claim 23

According to dependent claim 23, the server serves requests received from a user via the graphic user interface on a user's machine; the graphic user interface being for providing access functions and file editing functions (see page 5, lines 23-25 and page 7, lines 9-10).

Claim 24

According to dependent claim 24, the image server includes at least one selected from the group consisting of: a two dimensional image loader, a three dimensional image loader, a multi-media loader and a telemetry loader (see page 5, line 27-28).

Claim 25

According to dependent claim 25, the two-dimensional image loader is for retrieving two-dimensional still images (see page 5, line 30).

Claim 26

According to dependent claim 26, the three-dimensional image loader is for retrieving three-dimensional still images (see page 5, line 31).

Claim 27

According to dependent claim 27, the multi-media loader is for retrieving multi-media files (see page 5, line 32).

Claim 28

According to dependent claim 28, the telemetry loader is for retrieving telemetry data (see page 5, line 33).

Claim 29

According to dependent claim 29, the graphic user interface includes a PMIL client as a user interface able to run in a web browser or as a stand alone application on a user's machine, and provides MIRC editing functions (see page 5, lines 35-37 and page 7, lines 21-22).

Claim 30

According to dependent claim 30, the server includes an MIRC storage for providing an MIRC file storage service for the database and for the user's machine (see page 6, lines 1-2 and page 7, lines 24-25).

Claim 31

According to dependent claim 31, the MIRC server further includes an MIRC query to provide queries as defined by the MIRC scheme (see page 6, lines 2-3 and page 7, lines 25-26).

Claim 32

According to dependent claim 32, the at least one teaching file is in accordance with a Medical Imaging Resource Centre standard (see page 6, lines 6-7).

Claim 33

According to dependent claim 33, the formats of the medical images include at least one selected from the group consisting of: AVW, HDR/IMG (Analyze format version 8.0 and 7.5), BMP (Windows Bitmap format), DICOM (Digital Imaging and Communications in Medicine), GIF, JPEG, JPEG 2000, PNG, PNM, PPG, RGB, RGBA, SGI, TIFF, AVW, HDR/IMG (Analyze format: version 8.0 and 7.5), Animated GIF, MIRA, Mut-sliced TIFF, MOV, AVI, MP3, RM, and Waveform for ECG, EEG, EMG (see page 8, line 19-page 9, line 13).

Claim 34

According to dependent claim 34, all medical images are kept in their original format once retrieved (see page 9, lines 16-17).

Claim 35

According to dependent claim 35, for two-dimensional medical images, two additional JPEG images are generated for ease of browsing using a web browser; and for other image formats, an additional thumbnail image is generated (see page 9, lines 17-20).

Claim 36

According to dependent claim 36, the two additional JPEG images are of the same size as thumbnail images (see page 9, lines 18-19).

Claim 37

Claim 37 claims corresponding subject matter to claim 1 and is supported in the same sections of the specification.

Claim 37 describes a computer readable storage medium comprising a computer program code that, when executed, is configured to control a computer processor to retrieve medical images from various sources and in different formats; to enable the creation of teaching files and research datasets, for the building of a personal medical image library, by: directly retrieving a plurality of medical images from various sources; storing the plurality of medical images in a database; generating a database record for the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the teaching files and research datasets being compliant with at least one predetermined schema; saving the teaching files and research datasets into the database; generating at least one index of the teaching files and research datasets; and automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources. The patient identification data comprises patient sensitive information that is not revealed publicly. The automatic anonymizing of patient identification data includes replacing of each item of the patient identification data with an anonymization code. A relationship between the

anonymization code and the patient identification data is stored in a table securely in the database (see page 6, lines 9-11 and page 13, line 31-page 14, line 5).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-4, 6, 8-23, and 30-37 are unpatentable under 35 U.S.C. 103(a) over U.S. Patent No. 7,374,077 to Shimura (hereinafter " Shimura"), in view of U.S. Patent No. 7,080,098 to Smirniotopoulos et al., (hereinafter "Smirniotopoulos"), and further in view of U.S. Publication No. 2004/0139043 to Lei et al. (hereinafter "Lei").

Whether claims 24-29 are unpatentable under 35 U.S.C. §103(a) over Shimura in view of U.S.Publication No. 2003/0013951 to Stefanescu et al. (hereinafter "Stefanescu").

VII. ARGUMENT

Claim Rejections-35 U.S.C. §103(a)

For the purposes of this appeal, independent claims 1, 21, and 37 and those claims dependent thereon stand or fall together.

A. Introduction

In order to reject a claim under 35 U.S.C. § 103(a) it is necessary for the Examiner to lay out a valid, *prima facie* case of obviousness. This has not been done in the current case, because the cited references do not meet all of the limitations of the pending claims. When considering whether a claim is obvious, all of the limitations of the claim must be considered (see MPEP 2143.03). Because the references cited do not meet the limitations of the claims, no *prima facie* case of obviousness has been made, and the rejection of the claims under 35 U.S.C. § 103(a) should be withdrawn.

Shimura discloses an image search system comprising an image database which stores a number of pieces of image data representing a number of images; an image input means for inputting search image data representing the whole and/or a part of an image similar to which in feature is to be searched for; a searching means which searches the database for similitude image data representing an image which is similar to an image represented by the input search image data in feature; and a search report output means which outputs a search report representing result of search by the searching means (see Shimura, column 1, line 66 – column 2, line 12).

Smirniotopoulos discloses a multimedia medical database system including a multimedia database which stores within its secure table spaces the component tables in which the medical multimedia data is stored. The tables include a disease information or "factoid" table, an image/caption table, and a patient/clinical data table. This provides an interactive system for storing, retrieving and searching against a variety of medically relevant parameters. Multiple levels of privileges may be supported, such as for an author of a file, a reviewer, and editor, and a system administrator. When a user selects a process they want to use, the system may be designed to mask those processes or options within a given process, for which a user does not have sufficient privileges (see Smirniotopoulos, column 1, lines 46-61; column 2, lines 50-57; column 3, lines 37-39; and column 4, lines 5-7).

Lei discloses a method and apparatus for attribute relevant access control. A determination is made as to whether to modify a query based on which attributes of a database object are references in the query. If the query references one or more attributes of the database object that are restricted, the query may be modified based on attribute restriction metadata. Users are restricted from assessing data from the restricted attributes by masking the data before returning it to the users (see Lei, abstract, paragraphs [0023], [0024]).

Stefanescu discloses a database organization and searching system which provides techniques for organizing large-scale image data sources. Database records such as medical images may be pre-processed to effectively normalize data among different images. Each image, or a portion thereof, is then labeled according to some observed characteristic or other attributes. A model may then be trained to associate the feature vectors with the labels. The model is then

available for labeling other images. In this manner, searching techniques for well-organized or indexed databases may be applied automatically to databases that are not well-organized, but that have the same underlying data type (see Stefanescu, paragraph [0006]).

Claim 1 recites a method for retrieving medical images from various sources and in different formats, to enable the creation of teaching files and research datasets, for the building of a personal medical image library. The method comprises (a) directly retrieving a plurality of medical images from various sources; (b) storing the plurality of medical images in a database; (c) generating a database record for the teaching files and research datasets; (d) generating the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the teaching files and research datasets being compliant with at least one predetermined schema; (e) saving the teaching files and research datasets into the database; (f) generating at least one index of the teaching files and research datasets; (g) automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code. The method further comprises (h) securely storing a relationship between the anonymization code and the patient identification data in a table in the database.

B. <u>The combination of references does not disclose each and every feature as claimed in the independent claims</u>

None of the cited references discloses "securely storing a relationship between the anonymization code and the patient identification data in a table in the database" as recited in claim 1.

In claim 1, the problem of providing a simplified access control scheme for a database is solved by automatic anonymizing of patient identification data including replacing each item of the patient identification data with an anonymization code and securely storing a relationship between the anonymization code and the patient identification data in a table in the database. Patient specific information retrieved from the clinical image archive is very sensitive and can only be referenced internally. It is not allowed to appear in teaching files and datasets, which may be published. The automatic anonymizing of patient identification data in the method of claim 1 makes sure that the patient identification data is not revealed to the public in the teaching files and research datasets. At the same time, the method of claim 1 ensures the possibility to refer back to the actual patient when needed, by not simply removing the patient identification data from the teaching files and research datasets but securely storing a relationship between the anonymization code and the patient identification data in a table in the database. In this manner, a simplified access control scheme for the largest portion of the database is achieved, which saves computational resources. Additionally, securely storing the said relationship in a table in the database centralizes the sensitive information in a small core table that can be easily secured.

Shimura does not even disclose automatically anonymizing of patient identification data, let alone the anonymizing of patient identification data including replacing each item of the patient identification data with an anonymization code and the secure storing of a relationship

between the anonymization code and the patient identification data in a table in the database. This is as also acknowledged by the Examiner on page 4 and page 5 of the Office Action.

Smirniotopoulos discloses multiple levels of privileges supported by the system, such that those processes or options within a given process, for which a user does not has sufficient privileges, may be masked (see Smirniotopoulos, column 3, lines 37-39; and column 4, lines 5-7). However, Smirniotopoulos does not disclose anonymizing of patient identification data including replacing each item of the patient identification data with an anonymization code and the secure storing of a relationship between the anonymization code and the patient identification data in a table in the database. This is as also acknowledged by the Examiner on page 5 of the Office Action.

In the Office Action, it is stated at page 5, that "Lei teaches: wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code." Paragraph [0074], lines 7-9 through paragraph [0075] and paragraph [0076] of Lei (the replacing of the data from the attribute with the masking value of integer zero) are cited in the Office Action as allegedly teaching this feature. In addition, it is stated at page 5 of the Office Action that Lei teaches securely storing a relationship between the anonymization code and the patient identification data in a table in the database. Paragraph [0074], line 10 of Lei (the storing of the modified data in a masked result set) is cited in the Office Action as allegedly teaching this feature. These paragraphs, however, do not teach this feature, as will be discussed in the following.

Lei discloses that when a user inputs a query which references some attributes "NAME" and "SALARY", a database server obtains data for the requested names (non-sensitive information) and salaries (sensitive information) and stores this query result in a result set 235 (paragraphs [0031], [0064], [0074] of Lei). The query result, i.e. the result set 235, is masked by replacing the salary data of the restricted attribute with the masking value, integer zero, and the modified data is stored in a masked query result set 233 (e.g. Table 1) for output to the database application and eventually to the user (Figure 2, paragraph [0074] of Lei). The masking value may be an integer zero if the datatype of the restricted attribute is an integer; or may be a string of asterisks if the datatype of the restricted attribute is a string (paragraph [0052] of Lei); depending on the datatype of the restricted attribute. Therefore, the masking value has no relationship with the actual data (i.e. sensitive information) of the restricted attribute, but is related to the data type of the restricted attribute. According to Lei, for a restricted attribute "SALARY", regardless of the amount of salary, the masking value is an integer zero as shown in Table 2 of Lei. In other words, Lei does not even disclose defining a relationship between the masking value (anonymization code) and the salary (sensitive information), let alone providing any motivation to securely storing such a relationship in a table in the database.

In contrast, securely storing of a relationship between the anonymization code and the patient identification data in a table as recited in claim 1 of the present application would enable the retrieval of the patient identification data using the corresponding anonymization code in a secure way. However, Lei does not disclose or suggest storing such a relationship for possible retrieval of sensitive data later on. In fact, Lei discloses the result set 235 with both non-sensitive

information (name) and sensitive information (salary), and the masked result set 233 with sensitive information (salary) anonymized, stored in the database server 230. Because all the information are stored in the result set 235 and the masked result set 233 in the database server 230, there is no motivation to store an additional correspondence relationship between the masked value and the sensitive data. Therefore, Lei would not provide any motivation to securely store a correspondence relationship between the anonymization code and the sensitive data in a table.

In another aspect, according to the subject matter of pending claim 1, the relationship between the anonymization code and the patient identification data is stored in a table in the database, which is the same database as the one which stores the plurality of medical images. In Lei, the entire data containing sensitive information (which is not anonymized) is stored in the main database 240 (table 2), which has to be fully protected against unauthorized access attempts.

In contrast thereto, storing the relationship between the anonymization code and the patient identification data in a separate table in accordance with pending claim 1 allows securing only a small portion of the database instead of protecting the whole database as required in Lei. According to claimed method, the main portion of the database which has the medical images stored thereon does not need to be protected because the patient identification information is anonymized in the main database.

For the above reasons, Lei does not teach or suggest "securely storing a relationship between the anonymization code and the patient identification data in a table in the database," as recited in claim 1.

Therefore, because none of Shimura, Smirniotopoulos, and Lei teaches or suggests securely storing a relationship between the anonymization code and the patient identification data in a table in the database, as required by claim 1, as a result, there can be no basis for the rejection of claim 1 based thereon. Independent claim 1 therefore is patentable under 35 U.S.C. §103(a) over these references for at least these reasons.

C. One of ordinary skill in the art would not have been motivated to combine Shimura, Smirniotopoulos, and Lei to arrive at the invention as claimed in the independent claims.

The cited art fails to recognize the problem addressed by the subject-matter of claim 1.

Section B above describes specific deficiencies of the cited references, which are sufficient to overcome the rejections as set forth in the Office Action. However, the absence of the elements highlights clearly that the problems addressed by claim 1 are also completely outside the scope of the cited references.

By automatic anonymizing of patient identification data including replacing each item of the patient identification data with an anonymization code and by securely storing a relationship between the anonymization code and the patient identification data in a table in the database, the method of claim 1 provides a simplified access control scheme in which the patient identification data is not revealed to the public in the teaching files and research datasets and at the same time it can refer back to the actual patient when needed. In this manner, a simplified access control

scheme for the largest portion of the database is achieved, which saves computational resources and does not need to create and manage different levels of privileges for access. Additionally, securely storing the said relationship in a table in the database centralizes the sensitive information in a small core table that can be easily secured.

None of Shimura, Smirniotopoulos, and Lei is concerned with the problem solved by the method of claim 1.

Shimura is concerned with a system for similar image search. Shimura does not mention any problem of preventing revealing patient information to the public, and thus would not be concerned with the retrieving of patient information after having been anonymized.

Smirniotopoulos discloses multiple levels of privileges supported by the system, such that those processes or options within a given process, for which a user does not has sufficient privileges, may be masked. Smirniotopoulos is concerned with providing multiple levels of privileges to users, and is not concerned with retrieving the sensitive information after the masking.

Lei is concerned with controlling the access to restricted attribute by replacing the data of the restricted attribute with a masking value depending on the type of the restricted attribute. Lei is concerned with preventing revealing data of restricted attribute to a user without accessing right, but is not concerned with retrieving the data of the restricted attribute after the data of the restricted attribute has been masked. Thus, Lei would not provide any motivation to define and store a relationship between the masking value and the data of the restricted attribute, so as to retrieve the data of the restricted attribute based on the stored relationship.

In view of the above, as Shimura, Smirniotopoulos and Lei are concerned with different problems, there is no motivation to combine these references. In addition, none of Shimura, Smirniotopoulos and Lei is concerned with preventing revealing of sensitive information and at the time providing the possibility to retrieve the sensitive information which has been anonymized. Thus, even if the disclosure of Shimura, Smirniotopoulos and Lei were combined, they could not arrive at the method as claimed in pending claim 1, as the above feature of "securely storing a relationship between the anonymization code and the sensitive patient identification data in a table in the database" is neither taught nor suggested in these references.

For the reasons given above, independent claim 1 is patentable under 35 U.S.C. §103(a) over Shimura, in view of Smirniotopoulos and Lei.

Given that claims 2-4, 6, and 8-20 depend from independent claim 1 and add additional limitations, claims 2-4, 6, and 8-20 are patentable under 35 U.S.C. §103(a) over Shimura, in view of Smirniotopoulos and Lei for at least the same reasons. Therefore, Appellants request the withdrawal of the rejection of claims 2-4, 6, and 8-20 under 35 U.S.C. §103(a).

As set forth above, even if Shimura, Smirniotopoulos and Lei were combined, such a combination would still lack securely storing a relationship between the anonymization code and the sensitive patient identification data in a table in the database, as recited in independent claim 21.

Therefore, independent claim 21 is patentable under 35 U.S.C. §103(a) over Shimura, in view of Smirniotopoulos and Lei.

Given that claims 22-23, and 30-36 depend from independent claim 21 and add additional limitations, claims 22-23, and 30-36 are patentable under 35 U.S.C. §103(a) over Shimura, in view of Smirniotopoulos and Lei for at least the same reasons. Therefore, Appellants request the withdrawal of the rejection of claims 22-23, and 30-36 under 35 U.S.C. §103(a).

As set forth above, even if Shimura, Smirniotopoulos and Lei were combined, such a combination would still lack securely storing a relationship between the anonymization code and the sensitive patient identification data in a table in the database, as recited in independent claim 37.

Therefore, independent claim 37 is patentable under 35 U.S.C. §103(a) over Shimura, in view of Smirniotopoulos and Lei.

Claims 24-29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Shimura and further in view of U.S. Publication No. 2003/0013951 to Stefanescu.

As set forth above, even if Shimura, Smirniotopoulos and Lei were combined, such a combination would still lack securely storing a relationship between the anonymization code and the sensitive patient identification data in a table in the database, as recited in independent claim 21.

As set forth above, Stefanescu discloses a database organization and searching system. Stefanescu does not teach or suggest the feature of "securely storing a relationship between the anonymization code and the patient identification data in a table in the database", as recited in independent claim 21.

Given that claims 24-29 depend from claim 21, and add additional limitations, claims 24-29 are patentable under 35 U.S.C. §103(a) over Shimura in view of Smirniotopoulos, Lei and Stefanescu.

VIII. CONCLUSION

In summary, Appellants contend that a combination of the cited art cannot be used to render obvious the pending claims in the manner suggested by the Examiner. Therefore, Appellants respectfully submit that all appealed claims in this application are patentable and request that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due.

Respectfully Submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: June 22, 2011

/Tatiana Rossin/

Tatiana Rossin
Reg. No.: 56,833

1279 Oakmead Parkway
Sunnyvale, CA 94085
(408) 720-8300

Customer No. 08791

IX. CLAIMS APPENDIX

The claims involved in the appeal are as follows.

1. A method for retrieving medical images from various sources and in different formats, to enable the creation of teaching files and research datasets, for the building of a personal medical image library, the method comprising:

(a) directly retrieving a plurality of medical images from various sources;

(b) storing the plurality of medical images in a database;

(c) generating a database record for the teaching files and research datasets;

(d) generating the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the teaching files and research datasets being compliant with at least one predetermined schema;

(e) saving the teaching files and research datasets into the database;

(f) generating at least one index of the teaching files and research datasets;

(g) automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code; and

(h) securely storing a relationship between the anonymization code and the patient identification data in a table in the database.

2. The method as claimed in claim 1, further including a searching mechanism for searching the teaching files and research datasets.

3. The method as claimed in claim 1, wherein the medical images are from at least one discipline selected from the group consisting of: radiology, nuclear medicine, dermatology, pathology, ophthalmology, cardiology, neurology, endoscopy, angiography, biomedicine, ECG, EEG, and EMG.

4. The method as claimed in claim 1, wherein the method is in accordance with MIRC schema.

6. The method as claimed in claim 1, wherein the patient identification data is able to be revealed to a generator of the teaching files and research datasets.

8. The method as claimed in claim 1, wherein the anonymization code includes a prefix, a randomly generated number and a type.

9. The method as claimed in claim 8, wherein the prefix is a short string of characters

representing the generator of the sensitive information; and the type represents nature of the sensitive information.

10. The method as claimed in claim 1, wherein a check is first performed to determine if the item of sensitive information has previously been anonymized and the anonymization code previously generated; and, if yes, retrieving and using the previously generated anonymization code.

11. The method as claimed in claim 1, wherein the sensitive information includes one or more items selected from the group consisting of: patient's name, patient ID, other patient's names, other patient IDs, patient's birth name, patient's address, patient's telephone numbers, patient's mother's birth name, region of residence, country of residence, military rank, branch of service, patient comments, additional patient history, referring physician's name, referring physician's address, referring physician's telephone numbers, and all other person names.

12. The method as claimed in claim 1, wherein, in step (c), ACR codes are entered as a result of system prompts.

13. The method as claimed in claim 12, wherein the ACR codes are used for the at least one index of the teaching files.

14. The method as claimed in claim 1, wherein indexing is by at least one selected from the group consisting of: title, abstract, keywords, authors, affiliations, contacts, patient information, radiological codes, image format, image compression status, image modality, anatomic location, and ACR codes.

15. The method as claimed in claim 2, wherein, for internal searching, patient sensitive information is revealed, and for external searching patient sensitive information is anonymized.

16. The method as claimed in claim 1, wherein after each medical image is retrieved in step (a) it can be viewed before being stored.

17. The method as claimed in claim 1, wherein all medical images are kept in their original format once retrieved.

18. The method as claimed in claim 17, wherein the formats include at least one selected from the group consisting of AVW, HDR/IMG (Analyze format version 8.0 and 7.5), BMP (Windows Bitmap format), DICOM (Digital Imaging and Communications in Medicine), GIF, JPEG, JPEG 2000, PNG, PNM, PPG, RGB, RGBA, SGI, TIFF, AVW, HDR/IMG (Analyze format: version 8.0 and 7.5), Animated GIF, MIRA, Mut-sliced TIFF, MOV, AVI, MP3, RM, and Waveform for ECG, EEG, EMG.

19. The method as claimed in claim 18, wherein for two-dimensional medical images, two additional JPEG images are generated for ease of browsing using a web browser; and for other image formats, an additional thumbnail image is generated.

20. The method as claimed in claim 19, wherein the two additional JPEG images are of the same size as thumbnail images.

21. An apparatus for retrieving medical images from various sources and in various formats for creating at least one teaching file and research dataset; the apparatus comprising:

a database for storing the at least one teaching file and research dataset in a generated database record, an image retrieval interface configured to directly retrieve medical images from various sources and in different formats,

an MIRC server configured to provide an MIRC file storage service for the database and for a user's machine automatically anonymizing patient identification data based upon the at least one medical image retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, and wherein a relationship between the anonymization code and the patient identification data is stored securely in a table in the database;

a graphic user interface for operation on a user's machine to communicate with the MIRC server; and

a web server to service requests from the graphic user interface.

22. The apparatus as claimed in claim 21, wherein the database is a relational database for storage of all required information, including: database tables; database indexes; database scripts; and pointers to the medical images, teaching files and research datasets.

23. The apparatus as claimed in claim 21, wherein the server serves requests received from a user via the graphic user interface on a user's machine; the graphic user interface being for providing access functions and file editing functions.

24. The apparatus as claimed in claim 21, wherein the image server includes at least one selected from the group consisting of : a two dimensional image loader, a three dimensional image loader, a multi-media loader and a telemetry loader.

25. The apparatus as claimed in claim 24, wherein the two-dimensional image loader is for retrieving two-dimensional still images.

26. The apparatus as claimed in claim 24, wherein the three-dimensional image loader is for retrieving three-dimensional still images.

27. The apparatus as claimed in claim 24, wherein the multi-media loader is for retrieving multi-media files.

28. The apparatus as claimed in claim 24, wherein the telemetry loader is for retrieving telemetry data.

29. The apparatus as claimed in claim 21, wherein the graphic user interface includes a PMIL client as a user interface able to run in a web browser or as a stand alone application on a user's machine, and provides MIRC editing functions.

30. The apparatus as claimed in claim 21, wherein the server includes an MIRC storage for providing an MIRC file storage service for the database and for the user's machine.

31. The apparatus as claimed in claim 30, wherein the MIRC server further includes an MIRC query to provide queries as defined by the MIRC scheme.

32. The apparatus as claimed in claim 21, wherein the at least one teaching file is in accordance with a Medical Imaging Resource Centre standard.

33. The apparatus as claimed in claim 21, wherein the formats include at least one selected from the group consisting of: AVW, HDR/IMG (Analyze format: version 8.0 and 7.5), BMP (Windows Bitmap format), DICOM (Digital Imaging and Communications in Medicine), GIF, JPEG, JPEG 2000, PNG, PNM, PPG, RGB, RGBA, SGI, TIFF, AVW, HDR/IMG (Analyze format: version 8.0 and 7.5), Animated GIF, MIRA, Muti-sliced TIFF, MOV, AVI, MP3, RM, and Waveform for ECG, EEG, EMG.

34. The apparatus as claimed in claim 21, wherein all medical images are kept in their original format once retrieved.

35. The apparatus as claimed in claim 33, wherein for two-dimensional medical images, two additional JPEG images are generated for ease of browsing using a web browser; and for other image formats, an additional thumbnail image is generated.

36. The apparatus as claimed in claim 35, wherein the two additional JPEG images are of the same size as thumbnail images.

37. A computer readable storage medium comprising a computer program code that, when executed, is configured to control a computer processor to (a) retrieve medical images from various sources and in different formats; to enable the creation of teaching files and research

datasets, for the building of a personal medical image library, by: directly retrieving a plurality of medical images from various sources;

storing the plurality of medical images in a database;

generating a database record for the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the teaching files and research datasets being compliant with at least one predetermined schema;

saving the teaching files and research datasets into the database; generating at least one index of the teaching files and research datasets; and

automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing of each item of the patient identification data with an anonymization code, and wherein a relationship between the anonymization code and the patient identification data is stored securely in a table in the database.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.